Statement of Work (SOW)

Joint Staff J7 Engineering and Technology Services

15 April 2021

N0017819D8773 / N6600119F3600

1.0 INTRODUCTION

The Department of Navy (DoN), Naval Information Warfare Center Pacific, (NIWC Pacific) is acquiring technology and engineering services to support the Department of Defense (DoD) Joint Force Training and Development requirements. Specifically, NIWC Pacific Code 53629 will be supporting the Joint Staff J7 mission to train forces, develop doctrine, and provide an interoperable training environment to improve joint warfighter readiness for joint and multinational operations. This mission is accomplished within the distributed information infrastructure supporting military exercises, and joint warfighter training under the purview of Joint Staff J7.

1.1 SCOPE

The objective of this effort is to obtain the full range of technical and engineering services to assist and support NIWC Pacific to carry out its duties and responsibilities to support the delivery of Joint Force Training and Development for the Joint Staff J7 and its DoD, Coalition, and Agency partners. The range of services require subject matter expertise in specialized technology and engineering skill sets that match NIWC Pacific's need to meet the Joint Staff J7 requirements. These requirements include engineering design, network analysis and monitoring, integration of new technology into the operational environment, testing, trusted-agent Systems Administration for Radiant Mercury, and operation and maintenance of software, hardware and applications requirements.

The scope of services to be delivered includes engineering management functions such as configuration management, capability documentation and technical services, specialized technical services for military exercises and daily operations, infrastructure services and management, facilities engineering, network engineering, database management and application upgrades and integration services.

This is a level of effort (term), severable task order.

1.2 BACKGROUND

The Joint Staff J7, as the Chairman's lead for joint adaptive training, trains forces, develops doctrine, and provides an interoperable training environment to improve joint warfighter readiness for joint and multinational operations. This responsibility includes:

- Providing joint training systems that directly support the combatant commanders, Services, and defense agencies.
- Providing immersive training technologies including increased access to live, virtual, and constructive capabilities.

Growing complexity and increased number of training events along with an urgent need for increased fidelity of distributed/deployed support requires continuous planning and implementation of enhancements to the Joint Staff J7 global technical infrastructure. Failure to keep pace challenges an already strained workforce and risks mission failure if the Joint Staff J7 technical infrastructure does not deliver new/changed mission-essential capabilities needed to prepare joint fighting forces for real world operations.

2.0 APPLICABLE DIRECTIVES/DOCUMENTS

In the event of a conflict between the text of the SOW and the references cited herein, the text of this document shall take precedence. Nothing in this document, however, shall supersede applicable laws and regulations, unless a specific exemption has been obtained.

Document Type	No. / Version	Title
DODD	3020.26	Department of Defense Continuity Programs, January 2009
DOD MANUAL	5200.01 Volumes 1	DoD Information Security Program: Overview, Classification, And Declassification, dated February 24, 2012, Change 1 May 4, 2018
DOD MANUAL	5200.01 Volumes 2	DoD Information Security Program: Marking Of Classified Information,

		dated February 24, 2012, Change 2 March 13, 2013
DOD MANUAL	5200.01 Volumes 3	DoD Information Security Program: Protection Of Classified Information, dated February 24, 2012, Change 2 March 19, 2013
DOD MANUAL	5200.01 Volumes 4	DoD Information Security Program: Controlled Unclassified Information (CUI), dated February 24, 2012, Change 1 May 9, 2018
DOD	5220.22-M	National Industry Security Program Operating Manual (NISPOM), 28 February 2006, CH 2 18 May 2016
DODD	5220.22	National Industrial Security Program
DOD	5200.2-R	Personnel Security Program
DODI	8510.01	Risk Management Framework (RMF) for DoD Information Technology (IT)
DODD	8500.1E	DoD Directive – Information Assurance
DOD	5200.01-M	DoD Information Security Program
DOD MANUAL	5220.22	National Industrial Security Program: Industrial Security Procedures for Government Activities, 1 August 2018
DODD	8570.01-M	DoD Directive Information Assurance Workforce Improvement Program
DODI	8500.01	DoD Instruction – Cybersecurity, March 2014
DoDD	8140.01	Cyberspace Workforce Management, Aug 2015
CJCSM	3115.01C	Joint Data Network Operations Volume 1
CJCSI	3170.01 series	Capabilities Integration and Development System, May 2007
CJSI	6211.02D	Defense Information Systems Network (DISN) Responsibilities, January 2012
CJCSI	6212.01 series	Interoperability and Supportability of Information Technology and National Security Systems, March 2007
CJCSI	6510.01F	Information Assurance (IA) and Support to Computer Network Defense (CND)
CJCSM	3170.01 series	Operation of the Joint Capabilities Integration and Development System, May 2007
DON Regulation	SECNAVINST 5510.30	Personnel Security Program
	SECNAV Manual 5510.30	Department of Navy Personnel Security Program, June 2006
	SECNAVINST 5510.36B	DON Information Security Program, dated 12 July 2019
SPAWAR	Inst 3432.1	Operations Security Policy, 2 February 2005
Department of Defense Architectural Framework	DODAF 2.02	DoD Deputy Chief Information Officer
	National Security Decision Directive 298	National Operations Security Program (NSDD) 298, 22 January 1988
DOD	5205.02-M	DOD Operations Security (OPSEC) Program, 3 November 1988, Change 1, 26 April 2018
	OPNAVINST F3300.53C	Navy Antiterrorism Program
	OPNAVINST 3432.1	DON Operations Security, 4 November 2011
	SPAWARINST 3432.1	Operations Security Policy, 2 February 2005

3.0 PERFORMANCE REQUIREMENTS – BASE PERIOD

The contractor shall provide support services in the work areas listed below. Technical support tasks may require on-call/recall or overtime capacity during 24/7 events and mission rehearsals a minimum of three (3) times per year. Tier I, Tier II and Tier III support levels are defined as follows:

- **Tier I** - This is the initial support level responsible for basic customer issues. The first job of a Tier I specialist is to gather the customer's information and to determine the customer's issue by analyzing the symptoms and figuring out the underlying problem. Personnel at this level have a basic to general understanding of the product or service and may not always contain the competency required for solving complex issues.

- **Tier II -** This is a more in-depth technical support level than Tier I requiring an elevated level of experience and knowledge on a particular product or service. Technicians in this realm of knowledge are responsible for assisting Tier I personnel in solving basic technical problems and for investigating elevated issues by confirming the validity of the problem and seeking known solutions related to these more complex issues. If personnel from this group cannot determine a solution, they are responsible for consolidated all actions taken and elevating the issue to the Tier III technical support group.

- **Tier III -** This is the highest level of support in a three-tiered technical support model responsible for handling the most difficult or advanced problems. These individuals are experts in their fields and are responsible for not only assisting both Tier I and Tier II personnel, but with the research and development of solutions to new or unknown issues. Tier III engineering support is the principal focus of this tasking.

3.1 Information Systems, Cybersecurity, and Information Technology (IT) Support

The contractor shall provide support in accordance with the following paragraphs:

3.1.1 ***Approximately 50%*** of the level of effort for 3.1. *Information Systems Services Support*. The contractor shall provide engineering design, technology upgrades, integration, operation, and maintenance of the software, hardware and applications within the distributed information infrastructure supporting the Joint Staff J7, its training audiences, training sources, and training observers. This support includes all mission related servers (name, directory, messaging, application, web and collaboration), work-stations, data storage, backup/recovery, software applications, hardware platforms and operating systems required to enable robust and efficient information communications. Additionally, the contractor shall support JS J7 initiatives enabling a more scalable, secure, containerized and adaptable infrastructure using methodologies focused on integrating security, development, and operations (SECDEVOPS) into a single continuous process. Specifically, in support of this task the contractor shall:

a) Configure virtual machine templates with VMware ESXi and vCenter Server for both server and thin client deployments for Joint Staff J7 networks.
b) Provide VMware Certified Professional, and Tier III support to monitor, update, and troubleshoot multiple VMware environments, hosting hardware and products to include VMware vCenter and VMware Horizon View, during daily operations and during training events by coordinating with Tier I and Tier II support staff to ensure continuous operations.
c) Provide VMware design, installation, configuration, testing, integration, life cycle recommendations, documentation, Defense Information Systems Agency (DISA) STIG applications, troubleshooting, repair, monitoring and management of enterprise network services environments involving VMware and ACAS monitoring and compliance.
d) Provide installation, configuration changes, updates, and operation and maintenance of Microsoft System Center Configuration Manager (SCCM), providing reporting capability for hardware and software inventory, commercial application updates and removal, changes to registry entries, and installation of updated device drivers.
e) Provide certified Microsoft Exchange system administration to maintain, restore, archive, duplicate, troubleshoot, upgrade, search, extract messages and repair Exchange databases on internal and external Joint Training networks.
f) Deploy, maintain, troubleshoot, upgrade and repair Microsoft Application Virtualization (App-V) server. Create packages using the Application Virtualization Sequencer to be deployed across the environment to provide centralized application management and license control
g) Provide certified Microsoft SharePoint 2016 (or later release) systems administration to maintain, restore, duplicate, troubleshoot, upgrade and repair SharePoint sites and databases on internal and external Joint Training networks. Additionally, provide Tier III support for transfer, duplication and migration of sites from external farm installations in exercise and training environments.
h) In accordance with event requirements and DoD Cybersecurity directives, construct, harden, control and stage approved Windows and Joint Staff J7 application Operating System (O/S) load-configurations for distribution to all Joint Training Enterprise Network (JTEN), including game floor workstations. Configure O/S to prevent spillage to foreign nationals.
i) Provide design, installation, configuration, testing, integration, documentation, troubleshooting, repair, monitoring, and management of enterprise network services environments involving Microsoft Windows and VMware installations. This task includes, but is not limited to, rapid deployment, analysis of information system usage and data flows, evaluation/installation of new Operating Systems (O/S), O/S software patches, and commercial application updates, documenting network services configuration changes.

j) Resolve set up and installation issues related to Host-based Intrusion Prevention System (HIPS), McAfee Firewall, Security Technical Implementation Guide (STIG) requirements, Structured Query Language (SQL) Databases, Oracle, Postgres, Internet Information Server (IIS), Apache, Group Policy, Domain Name Server (DNS) & Whitelist entries, Secure Socket Layer (SSL), Transport Layer Security (TLS), Internet Protocol Security (IPsec) encryption, Infoblox, network and database connections.
k) Provide vulnerability assessments in support of network and application vulnerability scanning using Assured Compliance Assessment Solution (ACAS) for Joint Staff J7 networks.
l) Provide integration, configuration, operation, management, monitoring, troubleshooting, and documentation in support of the Host Based Security System (HBSS) using McAfee ePolicy Orchestrator (ePO) for Joint Staff J7 Networks.
m) Provide, installation, operation and maintenance of BrightMail and McAfee email/web security gateway virtual appliances.
n) Perform testing, troubleshooting, repair and maintenance actions and management for Joint Staff J7 systems including Vovici, Facilitate, and Joint Training Information Management System (JTIMS) Lite, JTIMS Enterprise.
o) Construct, document, configure, troubleshoot, upgrade and maintain a complete domain environment for commercial networks.
p) Provide hardware setup and configuration for hardware to include HP G7 and G8 blade-systems, HP C7000 and C3000 chassis, HP Flex-10 network modules, HP Virtual Connect, HP B-series Storage Area Network (SAN) Advisor, Brocade Fiber Channel Host Bus Adapters, Brocade SAN Switch, NetApp Fabric Attached Storage (FAS) Arrays, NetApp OnCommand System Manager and Teredici Zero Clients.
q) Perform monitoring, testing, troubleshooting, repair and maintenance actions and management of the Joint Staff J7 data center, servers, databases, web-applications and operating infrastructure across the enterprise services.
r) Compile and deliver technical documentation for configuration changes and upgrades as required to include, but not limited to, 'as-built' drawings/diagrams, test data matrices, and standard operating procedures (SOP) in accordance with Joint Staff J7 identified policy and best practices.
s) Provide Tier III engineering support throughout training events by coordinating and consulting with Tier I and II support staff and exercise controllers to identify and resolve network performance issues. This task may require scheduled shift work to accommodate the scheduled outages during non-productive or non-exercise work hours.

3.1.2 ***Approximately 15%*** of the level of effort for 3.1. *Information Systems - Audio/Video (AV) Systems Support*. The contractor shall provide distribution support, maintenance and repair of all Joint Staff J7 AV and Video Teleconferencing (VTC) assets. Specifically, in support of this task the contractor shall:

a) Perform engineering evaluation, upgrades, installation and system integration tests for AV hardware to include related software.
b) Provide exercise support for Joint Staff J7 events to include Tier III engineering, testing, upgrades, and technology insertion for various AV systems including tv broadcast studio infrastructure support for exercise stimulation.
c) Provide trained and certified AV Extron Electronics Subject Matter Experts (SMEs) for system design, build, and configuration support.
d) Coordinate with and train the AV operators on upgrades to Joint Staff J7 conferencing equipment to include, but not limited to, PESA Video/Audio routing switch, Cisco, and Extron.
e) Provide trained and certified SMEs to securely upgrade, configure, test, repair and maintain VTC systems, cable television systems, display devices (i.e. plasma and LCD monitors, projectors, etc.), cameras, AV matrix and distribution switches, servers, hubs, routers, telephone switches, encryption devices, fiber optic distribution systems and modems.
f) Provide on-call/recall technical support during 24/7 Joint Staff J7 events to identify and correct circuit / equipment discrepancies.
g) Coordinate and consult with Tier I and II support staff and event controllers to ensure equipment availability, optimal circuit quality and reliability during Joint Staff J7 events.
h) Document system configuration changes, update asset management reports and operational guidance documentation as required.

3.1.3 ***Approximately 10%*** of the level of effort for 3.1. *Information Systems – Command and Control (C2) Support*. The contractor shall provide advanced Security+ CE certified Command and Control (C2) system administration, engineering, and C2 software and hardware support with an emphasis on GCCS-J (Global Command and Control System – Joint), GCCS-I3 (Global Command and Control System – Integrated Imagery and Intelligence), GCCS-J Agile Client, Joint Range Extension (JRE), Tactical Data Analysis and Connectivity System (TDACS), Air Defense System Integrator (ADSI), Theater Battle Management Core System (TBMCS), Radiant Mercury Cross Domain Solution, North Atlantic Treaty Organization (NATO) C2 systems Integrated Command and Control (ICC), Joint Deployable Intelligence Support System (JDISS), and Maritime Command and Control Information System (MCCIS). Specifically, in support of this task the contractor shall:

a) Provide trained and certified Oracle Solaris Operating Systems, latest approved Windows OS (currently Windows 10) and Windows Server (currently Windows Server 2012), and latest approved Linux (currently Linux 6) systems administrators.
b) Provide and implement cybersecurity compliance of joint C2 systems by tracking, applying and validating Information Assurance Vulnerability Alert (IAVA) configuration changes per the direction of DISA GCCS-J Program Management Office and other C2 system program offices. Maintain all Command and Control Programs of Record, to include GCCS-J, ADSI, TDACS, JDISS and JRE systems, in accordance with DISA STIG.
c) Provide a system administrator trained and certified for the role of a system administrator for Radiant Mercury (RM) to perform tasks including, but not limited to, moving event data between security domains, creation and modification of RM accounts, review/archive/retrieve/define/delete message logging, lock/unlock configuration objects, review audits, perform system backups, install/uninstall data facility configuration files, and modify network internet protocol (IP) parameters.
d) Provide C2 SME input to Joint Live, Virtual, Constructive (JLVC) federation managers in order to provide Model & Simulation (M&S) interface recommendations and in-depth Common Operational Picture (COP) track data understanding and knowledge to provide a realistic COP environment to the joint training audience.
e) Perform interoperability analyses, develop integration designs, and provide recommendations for joint training C2 architecture development, upgrades, modifications, or alterations of hardware and software as appropriate to improve system operations and to enhance the security posture of the Joint Staff J7 C2 Programs of Record in the joint training environment.
f) Provide technical engineering and operational support for Joint Staff J7 Joint C2 program requirements, design and integration of multiple joint C2 system architectures on the JTEN and multiple Coalition networks across various organizations (Joint, Service, DoD, Coalition partners, non-DoD agencies) in the CONUS and OCONUS.
g) Analyze new and existing C2 systems and equipment performance issues (i.e. analyze C2 system network performance, C2 system usage and data flows, C2 system interfaces, C2 system transmission techniques and protocols) for interfacing with other C2 or model and simulation systems.

3.1.4 ***Approximately 5%*** of the level of effort for 3.1. *Information Systems – Modeling and Simulation (M&S) Support.* The contractor shall provide engineering, analytical and technical services plus incidental management and administrative efforts in support of the development, design, analysis and implementation of modeling and simulation techniques supporting unique military applications at Joint Staff J7. This includes but is not limited to support for the sponsor-owned federation of Service/Joint developed models (i.e. JLVC) and testing of various interface standards. Specifically, in support of this task, the contractor shall:

a) Assess and test the interoperability of M&S software and applications with C2 and network components for compatibility with complex mission specific requirements, and validate proper interface within the Joint Staff J7 and JTEN infrastructure.
b) Provide M&S design, development, testing and integration support to the Joint Staff J7 for acceptability in the future JLVC releases.
c) Develop and maintain model hierarchy, relationships and dependencies, including supporting documentation and plans.
d) Provide problem resolution, revision, and maintenance of modules of M&S hardware and applications.
e) Participate in technical working groups to analyze and determine operational parameters for modeling architecture.
f) Provide M&S management support to the deployment and system support teams for the deployment and installation of joint M&S systems.

3.1.5 ***Approximately 5%*** of the level of effort for 3.1. *Cybersecurity Support*. The contractor shall provide the necessary cybersecurity technical support for the Joint Staff J7 to design, build, test, and implement its systems and networks. Specifically, in support of this task the contractor shall:

a) Develop and maintain Assessment and Authorization (A&A) documentation (Formerly Certification and Accreditation), create and/or maintain all A&A documentation to include, but not limited to, Configuration Management (CM) baselines, Risk Management Framework (RMF) documentation, security reviews and assessments, Plan of Action and Milestones (POA&Ms), post accreditation documentation, and other security documents as required by the Joint Staff's Operational Designated Approving Authority (ODAA).
b) Manage the A&A effort. A&A must be performed in accordance with the latest DoD Instruction for RMF 8510. The contractor shall execute all steps necessary for obtaining accreditations and maintaining complete A&A packages for all assigned systems and sites.
c) The contractor shall support, initiate and track A&A meetings. The contractor shall maintain A&A meeting agendas, minutes and action items. All A&A documents shall be posted in a Joint Staff J7 designated controlled centralized area.
d) The contractor shall define security requirements and support evaluations, and must provide detailed recommendations on any current and new IT development efforts to ensure an efficient, successful A&A process.

e) The contractor shall provide RMF implementation support for Joint Staff J7 information systems and networks.

3.1.6 ***Approximately 5%*** of the level of effort for 3.1. *Cyber Security Engineering.* The Contractor shall serve as security advisor to the Government in all aspects of Cybersecurity and RMF to ensure JS J7 mission and programs, including non-CE2T2 (COCOM Exercise Engagement and Training Transformation), meet all requirements to support the J7 mission. These aspects include but are not limited to RMF, identifying and researching vulnerabilities, performing risk analysis and recommending and mitigating controls, performing system Information Assurance Vulnerability Management (IAVM) and STIG compliance audits, and provide cyberspace defense support to Joint Staff J7. In providing Cybersecurity support the contractor shall support Information Assurance Management (IAM) Level III tasks to include:

a) Provide Subject Matter Expertise to aid Program Managers in the development of A&A documentation.
b) Perform a technical review of A&A documentation for compliance with applicable DoD and Joint Staff cybersecurity policies.
c) Assess security compliance, support program security reviews, and coordinate and compile security-related documentation.
d) Assist with the preparation and revision of J7 cybersecurity policy and guidance documents for specific cybersecurity related technologies.
e) Provide critical written and oral analysis of security architecture documentation and vulnerability and risk assessments.
f) Assist in the development of plan of actions and milestones (POA&M) and tracking of milestones within POA&Ms directly related to cybersecurity requirements.
g) Perform validation of cyber security controls in support of assessment and authorization efforts.
h) Coordinate with system owners to ensure the appropriate A&A artifacts are developed to support system authorization.
i) Develop IT sustainment documents and actions and renewal documentation is resident in the database.
j) Provide security incident reports as required outlining the specific security issue, critical concerns, and remediation actions required to resolve or mitigate the issue.

3.1.7 ***Approximately 5%*** of the level of effort for 3.1. *Information Technology – Data Center Management Support*. The contractor shall provide the engineering necessary for proper design, infrastructure upgrades, testing, maintenance oversight, and operational readiness and restoral of data center power infrastructure. Specifically, in support of this task the contractor shall:

a) Provide Power Systems Subject Matter Expert to ensure the proper operational readiness of multiple data center power infrastructures.
b) Provide monitoring of overall systems power status, analyze the engineering design of multiple Uninterruptible Power Supply (UPS) systems, coordinate routine preventive maintenance (e.g. load-testing, switch testing), attend design review meetings and working groups to ensure adequate power resources are planned to be available, and provide system design, infrastructure upgrades, testing, operational readiness and restoral.
c) Provide power monitoring expertise to manage data center specific power monitoring networks that report power consumption to the rack unit level.
d) Monitor power systems status; review and request updates to the building owners maintenance processes and disaster recovery plan to ensure situational as well as operational readiness.
e) Evaluate engineering designs of new and existing uninterruptible power system (UPS) to ensure adequate electrical power for new and existing critical IT Joint Staff J7 training equipment is accounted for as part of future planning.
f) Provide Liaison with Joint Staff J7 physical security, facility, property management, commercial electrical distribution personnel and government representatives during power system restoral/disaster recovery processes.
g) Coordinate with the building owners representative for scheduled maintenance and routine preventive maintenance (e.g. load-testing, switch testing) to ensure equipment availability during restoral.
h) Develop the acceptance and restoral sequences of power system installations or outage processes to ensure the reliability of power switchovers.
i) In support of the above tasks, provide on-call/recall status beyond normal working hours and shift work to accommodate scheduled outages during non-productive work hours.
j) Construct, document, configure, troubleshoot, upgrade and maintain hardware for deployable data centers.

3.1.8 ***Approximately 5%*** of the level of effort for 3.1. *Information Technology - Network Support.* The networks shall include, but are not limited to, the multiple local and wide area networks (LAN/WANs) of the Joint Training Enterprise Network (JTEN) Unclassified and SECRET, Joint Staff Zone D, and various Coalition Wide Area Networks (COWANs). The contractor shall provide analysis, design, integration, configuration, operation, maintenance, monitoring, testing, troubleshooting, documentation and management for the networks. Specifically, in support of this task, the contractor shall:

a) Set up, configure, install and integrate network devices to include routers, switches, virtual switches, servers, network appliances and PCs.

b) Perform password management and authentication, authorization and audit (AAA), device configuration resets and restore equipment to default settings at completion of exercises.
c) Provide network configuration changes, documentation/drawings, asset management and cable plant changes, IP management and documentation to maintain configuration control.
d) Integrate both software and hardware assets into the existing operation network without causing network disruptions.
e) Provide physical infrastructure support (cable & fiber plant) design, installation, fault location and maintenance.
f) Monitor operational status of the network and the network devices using various monitoring software applications and take independent corrective action to resolve performance degradation.
g) Provide network modeling and monitoring (e.g., Solar Winds), and perform network performance testing (i.e. bandwidth, packet loss, transfer time, packet analysis) and independently analyze and interpret results.
h) Analyze network for optimization including usage, traffic flows, bandwidth considerations, accesses and interfaces, transmission techniques, and protocols for proper interface with computer systems and user applications.
i) Provide Tier III exercise support by coordinating and consulting with Tier I and II support staff and exercise controllers to identify and resolve network performance issues. Coordinate and install technology updates and upgrades (Government furnished) during scheduled outages. This task may require scheduled shift work to accommodate the scheduled outages during non-productive or non-exercise work hours.
j) Test and verify interoperability of IOS software and hardware upgrades, IAVAs and security configurations, patches and updates with all current network devices and configurations, and stage configuration updates for centralized deployment to all network devices, including remote devices.
k) Participate in network design working groups to provide analysis and recommendations for network improvements, enhancements and upgrades. Consult with end-users, managers, and senior staff to ensure that deficiencies and alternatives have been fully identified and that network solutions will meet requirements.

3.2 Program Support

3.2.1 Department of Defense Architecture Framework (DODAF) Support. The contractor shall provide DODAF and other architecture support for the Joint Staff J7 to include the Joint Training Enterprise Architecture, simulated and real-world events (local, remote, distributed, live, virtual, and constructive; friendly, neutral, and threat forces). These tasks include, but are not limited to: concept development, planning, scheduling, logistics, modeling, simulation architecture design, simulation model management and operations, around-the-clock simulation pipeline operations, intelligence, scenario development, database builds and tests, distributed learning, courseware development, event response and control cells, assessment, and facility operations, as well as development of future joint training environments and the test and evaluation of proposed new equipment using the existing joint training environment resources. Specifically, in support of this task the contractor shall:

a) Provide subject matter expertise for the development of the Joint Capabilities Integration and Development System (JCIDS) compliant analysis and documentation. This will include supporting and providing input to existing program documentation as well as performing capability-based assessment and costing approaches for the evaluation of new technologies and modernization efforts.
b) Assist in the development, review, portfolio analysis, and coordination of Navy and Joint programs across the Joint Net-Centric Operations (JNO) Portfolio as it relates to DoD modernization initiatives.
c) Assist in the preparation and development of technical inputs for presentation material, technical information, and other capability documentations.
d) Provide subject matter expertise to the development and approval of required capability documents through Navy and Joint staffing processes within the National Capital Region. This includes technical support for the development of required document packages and senior leadership presentations.
e) Provide technical support for the development and/or update of existing architecture products within the DoD Architecture Framework (DoDAF) structure required to support the Network Ready Key Performance Parameter (NR KPP) for various components of modernization initiatives and programs.

3.3 Software Engineering, Development, and Programming Support

3.3.1 Software Engineering, Development, Programming Support. The Joint Staff J7 develops and hosts a variety of software applications running on a variety of platforms and software architectures. These include, but are not limited to, the Joint Event Management Information System (JEMIS), JS Security Database, Account Management, Asset Management, Enterprise Helpdesk, and Visitor In-processing and Patch Request software.

The contractor shall provide full life cycle software engineering and network support. Specifically, in support of this task the contractor shall:

a) Provide requirements analysis, design, development, testing, implementation and integration of software applications using open industry standard support software including but not limited to Eclipse, Subversion, Apache/Tomcat.

b) Support the integration of unique customer-applications utilizing Java, Oracle, Postgres, enterprise DB, as well as other software languages and technologies into the enterprise.
c) Provide full software life cycle system documentation and user training for each software application developed and implemented.
d) Provide Oracle and Postgres, and Enterprise DB Server Database Administration.
e) Coordinate with armed service representatives within the training community to determine requirements and ensure interoperability and integration of software, COTS appliances, as well as all required supporting enterprise services in the environment.

3.4 Software Engineering Approach

The contractor shall define a software development approach appropriate for the computer software effort to be performed under this solicitation. This approach shall be documented in a Software Development Plan (SDP) (CDRL A006). The contractor shall follow this SDP for all computer software to be developed or maintained under this effort.

The SDP shall define the offeror's proposed life cycle model and the processes used as a part of that model. In this context, the term "life cycle model" is as defined in IEEE/EIA Std. 12207.0. The SDP shall describe the overall life cycle and shall include primary, supporting, and organizational processes based on the work content of this solicitation. In accordance with the framework defined in IEEE/EIA Std. 12207.0, the SDP shall define the processes, the activities to be performed as a part of the processes, the tasks which support the activities, and the techniques and tools to be used to perform the tasks. Because IEEE/EIA Std. 12207 does not prescribe how to accomplish the task, the offeror must provide this detailed information so the Government can assess whether the offeror's approach is viable.

The SDP shall contain the information defined by IEEE/EIA Std. 12207.1, section 5.2.1 (generic content) and the Plans or Procedures in Table 1 of IEEE/EIA Std. 12207.1. In all cases, the level of detail shall be sufficient to define all software development processes, activities, and tasks to be conducted. Information provided must include, as a minimum, specific standard, methods, tools, action, strategies, and responsibilities associated with development and qualification.

4.0 PERFORMANCE REQUIREMENTS – OPTION PERIOD 1

Performance for option period 1 will be identical to base period 3.0.

5.0 PERFORMANCE REQUIREMENTS – OPTION PERIOD 2

Performance for option period 2 will be identical to base period 3.0.

6.0 PERFORMANCE REQUIREMENTS – OPTION PERIOD 3

Performance for option period 3 will be identical to base period 3.0.

7.0 PERFORMANCE REQUIREMENTS – OPTION PERIOD 4

Performance for option period 4 will be identical to base period 3.0.

8.0 CYBER SECURITY WORKFORCE

See SOW Addendum for updated CYBERSECURITY language.

9.0 Negligent Discharge of Classified Information (NDCI)

Negligent Discharge of Classified Information (NDCI). When information is placed on or processed on an information system with insufficient security controls to appropriately protect it (e.g., classified data on an unclassified system) there is a potential for an unauthorized disclosure. Such actions will be classified as a security violation, specifically a negligent discharge of classified information or NDCI. NDCI Cleanup actions may include the following actions:

i. Server destruction
ii. Hard drive wipe and destruction
iii. Containment actions

10.0 TRAVEL

10.1 Travel – Base Period

All travel is estimated to originate in the Suffolk, VA area (estimated place of performance).

The following travel is estimated for performance of the Base Period requirements. The below travel is also estimated for each option period. This is an estimate only:

Origin	Destination	# trips	# days	# people
Suffolk, VA	Washington D.C.	3	3	2
Suffolk, VA	Korea (OCONUS JTEN sites)	1	6	2
Suffolk, VA	Colorado Springs, CO (CONUS JTEN sites)	1	5	1
Suffolk, VA	Grafenwoehr, Germany	1	6	1

The contractor shall provide a trip report for each distinct trip as delineated in CDRL Data Item A008, Project Report, in the format prescribed by the COR.

10.2 Travel – Option Periods

Estimated travel for option periods 1, 2, 3 and 4 will be identical to base period 10.1. It is an estimate only.

OCONUS travel security requirements

The nature of this task requires access up to TS/SCI information. The work performed by the contractor will include access up to TS/SCI data, information, and spaces. The contractor will be required to attend meetings classified up to the TS/SCI. The contractor will be required to access SIPRnet, JWICS, COMSEC information, and NATO information.

IMPORTANT NOTE: SCI access will be required of the awardee after determination/validation by the IRCCO and the DD254 validation by either SSO Navy or its representative.

1. If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to Commanding Officer, Attn: Foreign Travel Team, Naval Information Warfare Center Pacific (NIWC Pacific), 53560 Hull Street, Building 27, 2nd Floor -Room 206, San Diego, CA 92152 for action. A Request for Foreign Travel form shall be submitted for each traveler, in advance of the travel, to initiate the release of a clearance message at least 30 days in advance of departure. Each Traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/Force Protection briefing within one year of departure and a country specific briefing within 90 days of departure.

2. Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is available at Joint Knowledge Online (JKO): https://jkodirect.jten.mil (prefix): course number: US007; title: Level 1 Anti-terrorism Awareness Training, if experiencing problems accessing this website contact the JKO Help Desk (24 hours a day/7 days a week, jkohelpdesk@jten.mil, 757-203-5654). The website will allow contractors who do not have a CAC to access the training. Sere 100.2 Level A code of conduct training is also required prior to Oconus travel for all personnel. Sere 100.2 Level A training can be accessed at http://jko.jfcom.mil (recommended), https://jkodirect.jten.mil/atlas2/faces/page/login/login.seam, recommended course: prefix: J3T: course #: A-US1329, for civilian, military, and contractors. Personnel utilizing this site must have a CAC or contractor shall request a sponsored account to access the training. Specialized training for specific locations, such as SOUTHCOM human rights, or U.S. forces Korea entry training, may also be required; NIWC Pacific security personnel will inform you if there are additional training requirements.

   Finally, EUCOM has mandated that all personnel going on official travel to the EUCOM AOR must now register with the Smart Traveler Enrollment Program (STEP). When you sign up, you will automatically receive the most current information the State Department compiles about your destination country. You will also receive updates, including Travel Warnings and Travel Alerts. Sign up is one-time only, after you have established your STEP account, you can easily add official or personal travel to anywhere in the world, not just EUCOM.
   http://travel.state.gov/content/passports/en/go/step.html

3. The contractor shall be familiar with and comply with the requirements, terms and conditions of the Status of Forces Agreement (SOFA) between the United States and any country in which travel requirements may arise under this effort.

11.0 SECURITY

11.1 Security

The nature of this task requires access to Top Secret (TS)/Sensitive Compartmented Information (SCI). The work performed by the Contractor will include access to unclassified and up to TS/SCI data, information, meetings, and spaces. The Contractor will be required to attend meetings classified up to the TS/SCI level. The Contractor will require access to Communications Security (COMSEC) and Secure Internet Protocol Router Network (SIPRNet).

IMPORTANT NOTE: SCI access will be required of the awardee after determination/validation by the IRCCO and the DD254 validation by either SSO Navy or its representative.

Although there is no requirement for the contractor to access NATO on this contract per Naval Intelligence Security Policy Directive 17-008 those contractors that have SCI access and those cleared SCI with JWICS or SIPRnet accounts shall be North Atlantic Treaty Organization (NATO) read-on and complete the derivative classification training prior to being granted access to JWICS/SIPRnet; training is provided by the facility security officer. Specific requirements provided in the Department of Defense Contract Security Classification Specification, DD Form 254.

Contractors performing tasks at the TS or below level without SCI access shall only receive the North Atlantic Treaty Organization (NATO) awareness brief and complete the derivative classification training prior to being granted access to SIPRnet; training is provided by the facility security officer.

Contractor personnel assigned to this effort who require access to SCI data and spaces must possess a current SSBI with ICD 704 eligibility (which replaced DCID 6/4 eligibility).

11.2 Operations Security (OPSEC)

OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or Critical Program Information, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD254.

12.0 OTHER

12.1 Property Requirements
Government Furnished Property (GFP) is not anticipated at this time.
Government Furnished Information (GFI) is not anticipated at this time.
Government Property (Incidental) is not anticipated at this time.
Government Furnished Facilities is not anticipated at this time.
Contractor Acquired Property (CAP) is not anticipated at this time.

12.2 Data Deliverables
Data deliverables shall be reviewed in accordance with the Department of the Navy Policy on Digital Product/Technical Data, Assistant Secretary of the Navy for Research, Development and Acquisition, ASN (RDA), memo of 23 October 2004, and as specified in the Contract Data Requirements List (CDRL) for this task order. The contractor shall provide a monthly status report to include in progress reviews, artifacts, and customer briefs, as required. All software source code and documentation will be uploaded and stored in the project Intelink repository or any other tool/environment the Government deems necessary based

(End of SOW)

SOW Addendum

I. TECHNICAL DIRECTION

(a) Technical Direction may be provided to the contractor from time to time by the Contracting Officer or Contracting Officer's Representative, if authorized, during the term (term is defined as the period of performance for the basic contract and any options that may be exercised) of this contract. Technical Direction will provide specific information relating to the tasks contained in the Statement of Work and will be provided to the contractor in writing. Any Technical Direction issued hereunder will be subject to the terms and conditions of the contract. RThe contract shall take precedence if there is any conflict with any Technical Direction issued hereunder, and cannot be modified by any Technical Direction.

(b) As stated, Technical Direction shall be issued in writing and shall include, but not be limited to:

(1) date of issuance of Technical Direction;
(2) applicable contract number;
(3) technical direction identification number;
(4) description of Technical Direction;
(5) estimated cost;
(6) estimated level of effort by labor category; and
(7) signature of the PCO or COR.

(c) If the contractor does not agree with the estimated cost specified on the technical direction, or considers the technical direction to be outside the scope of the contract, it shall notify the PCO or COR immediately and, in the case of the estimated cost, arrive at a general agreement to the cost of the task. In the case of the direction requiring work that is out of the scope of the contract, the contractor shall not proceed with the effort unless and until the PCO executes a contract modification to include the change in scope.

II. REPORTING REQUIREMENTS FOR CONTRACTED SERVICES

(NOTE: REPLACES PRIOR SOW PARAGRAPH 12.3 FOR OBSOLETE ECMRA LANGUAGE. THIS NEW INSTRUCTION IS ONLY APPLICABLE IF TASK ORDER MEETS REPORTING CRITERIA. CONTRACTOR TO CHECK REPORTING CRITERIA)

Services Contract Reporting (SCR) requirements apply to this contract. The contractor shall report required SCR data fields using the SCR section of the System for Award Management (SAM) at following web address: https://sam.gov/SAM/.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://sam.gov/SAM/.

III. CYBERSECURITY

Cybersecurity (which replaced the term Information Assurance (IA)) is defined as prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DON/Navy cybersecurity requirements.

Cyber IT and Cybersecurity Personnel

(a) The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M prior to accessing DoD information systems. Proposed contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the contract performance period or before assignment to the contract during the course of the performance period.

(b) The contractor shall be responsible for identifying, tracking and reporting cybersecurity personnel, also known as Cybersecurity Workforce (CSWF) and Cyber IT workforce personnel. Although the minimum frequency of reporting is monthly, the task order can require additional updates at any time.

(c) Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR) – Navy form as documented in para 8.2.2.4(b).

When a contractor requires logical access to a government IT system or resource (directly or indirectly), the required CAC will have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-M-V1, CAC PKI certificates will be associated with an official government issued e-mail address (e.g., .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the NIWC Pacific Information Assurance Management (IAM) office:

1. For annual DoD Cybersecurity/IA Awareness training, contractors shall use this site: https://twms.nmci.navy.mil/. For those contractors requiring initial training and do not have a CAC, contact the NIWC Pacific IAM office. Training can be taken at the IAM office or online at http://iase.disa.mil/index2.html.
2. For SAAR-N form, the contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form from the NIWC Pacific IAM office or from the website: https://navalforms.documentservices.dla.mil/.

(d) Contractor personnel with privileged access will be required to acknowledge special responsibilities with a Privileged Access Agreement (PAA) IAW SECNAVINST 5239.20A.

Design, Integration, Configuration or Installation of Hardware and Software

The contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the cybersecurity requirements as specified under DoDI 8500.01. The contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DON/Navy cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum:

Acceptable Use of Department of the Navy Information Technology (IT) dated 12 Feb 16. Use of blacklisted software is specifically prohibited and only software that is registered in DON Application and Database Management System (DADMS) and is Functional Area Manager (FAM) approved can be used as documented in para 5.2.2. Procurement and installation of software governed by DON Enterprise License Agreements (ELAs) – Microsoft, Oracle, Cisco, Axway, Symantec, ActivIdentity, VMware, Red Hat, NetApp, and EMC shall be in accordance with DON CIO Policy and DON ELAs awarded.

Cybersecurity Workforce (CSWF) Report

DoD 8570.01-M and DFARS PGI 239.7102-3 have promulgated that contractor personnel shall have documented current cybersecurity certification status within their contract. The contractor shall develop, maintain, and submit a CSWF Report as applicable at the task order level. IAW DFARS clause 252.239-7001, if cybersecurity support is provided, the contractor shall provide a Cybersecurity Workforce (CSWF) list that identifies those individuals who are IA trained and certified. Utilizing the format provided at the task order level, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Contractor shall verify with the COR or other government representative the proper labor category cybersecurity designation and certification requirements.

Contractors Performing Information Technology/Information System (IT/IS) administration and requiring elevated privileges on automated information system devices will be required to maintain an Information Assurance Technology (IAT) level two certification on all systems they administer. This would require individuals to obtain the following certifications based on their job function: Microsoft Windows Operating Systems (Client & Server), Microsoft Exchange, Microsoft Share Point Portal Server, Microsoft SQL Server, Microsoft Certified Professional, Microsoft, Certified Technical Specialist, Oracle, Cisco Network Devices, Juniper Network Devices, Security+, CISSP, and Extron Certified Installer.

The contractor shall be a Fully Qualified Navy Validator to support cybersecurity tasks at time of award.

Information Technology (IT) Services Requirements

This paragraph only applies to IT contracts. Information Technology (IT) is defined as any equipment or interconnected system(s) or subsystem(s) of equipment that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data of information by the agency. IT includes computers, ancillary equipment, peripherals, input, output, and storage devices necessary for security and surveillance. Electronic and Information technology (EIT) is IT that is used in the creation, conversion, or duplication of data or information. EIT includes: telecommunication products, such as telephones; information kiosks; transaction machines; World Wide Web sites; multimedia (including videotapes); and office equipment, such as copiers and fax machines.

Information Technology (IT) General Requirements

When applicable, the contractor shall be responsible for the following:

• Ensure that no production systems are operational on any RDT&E network.
• Follow DoDI 8510.01 of 12 Mar 2014 when deploying, integrating, and implementing IT capabilities.
• Migrate all Navy Ashore production systems to the NMCI environment where available.
• Work with government personnel to ensure compliance with all current Navy IT & cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).
• Follow SECNAVINST 5239.3B of 17 June 2009 & DoDI 8510.01 of 12 Mar 2014 prior to integration and implementation of IT solutions or systems.
• Register any contractor-owned or contractor-maintained IT systems utilized on contract in the Department of Defense IT Portfolio Registry (DITPR)-DON.
• Only perform work specified within the limitations of the task order.

Acquisition of Commercial Software Products, hardware, and Related Services

This paragraph only applies to the purchasing/hosting of commercial software. Contractors recommending or purchasing commercial software products, hardware, and related services supporting Navy programs and projects shall ensure they recommend or procure items from approved sources in accordance with the latest DoN and DoD policies.

DON Enterprise Licensing Agreement/DOD Enterprise Software Initiative Program

Pursuant to DoN Memorandum – Mandatory use of DoN Enterprise Licensing Agreement (ELA) dated 22 Feb 12, contractors that are authorized to use Government supply sources per FAR 51.101 shall verify if the product is attainable through DoN ELAs and if so, procure that item in accordance with appropriate ELA procedures. If an item is not attainable through the DoN ELA program, contractors shall then utilize DoD Enterprise Software Initiative (ESI) program (see DFARS 208.74) and government-wide SmartBuy program (see DoD memo dated 22 Dec 05). The contractor shall ensure any items purchased outside these programs have the required approved waivers as applicable to the program. Software requirements will be specified at the task order level.

DON Application and Database Management System

The contractor shall ensure that no Functional Area Manager (FAM) disapproved applications are integrated, installed or operational on Navy networks. The contractor shall ensure that all databases that use database management systems (DBMS) designed, implemented, and/or hosted on servers and/or mainframes supporting Navy applications and systems be registered in DoN Application and Database Management System (DADMS) and are FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DADMS and approved by the FAM. No operational systems or applications will be integrated, installed, or operational on the RDT&E network.

Section 508 Compliance

This paragraph only applies to IT contracts. The contractor shall ensure that all software recommended, procured, and/or developed is compliant with Section 508 of the Rehabilitation Act of 1973, 26 CFR Part 1194 and pursuant to SPAWARINST 5721.1B of 17 Nov 2009. In accordance with FAR 39.204, this requirement does not apply to contractor acquired software that is incidental to the task, software procured/developed to support a program or system designated as a National Security System (NSS) or if the product is located in spaces frequented only by service personnel for maintenance, repair or occasional monitoring of equipment.

Software Development/Modernization and Hosting

This paragraph only applies to software development and modernization. The contractor shall ensure all programs utilizing this contract for software development/ modernization (DEV/MOD), including the development of IT tools to automate NIWC Pacific business processes are compliant with DON Information Management/Information Technology (DON IM/IT) Investment Review Process Guidance requirements. Contractors shall neither host nor develop IT tools to automate NIWC Pacific business processes unless specifically tasked within the task order or contract. The contractor shall ensure IT tools developed to automate NIWC Pacific business processes will be delivered with full documentation and source code, as specified at the task order level, to allow non-proprietary operation and maintenance by any source. The contractor shall ensure all programs are submitted with proof of completed DEV/MOD certification approval from the appropriate authority in accordance with DON policy prior to task order award. *Note must be listed on Investment Review Board (IRB) approved list.

Information Security

Pursuant to DoDM 5200.01 and DoD 5200.48, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on contract. The contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

IT Position Designations

Pursuant to DoDI 8500.01, DoD 8570.01-M, SECNAVINST 5510.30, SECNAV M-5239.2, and applicable to unclassified DoD information systems, a designator is assigned to certain individuals that indicates the level of Special-Sensitive (SS)/Critical-Sensitive (CS) or Noncritical Sensitive (NCS), access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Per SECNAVINST 5510.30C, page 7, Section 8.b of enclosure (4), the Information Systems Security Manager is responsible for establishing, implementing and maintaining the DoN information system and information assurance program and is responsible to the Commanding Officer for developing, maintaining, and directing the implementation of the Information Assurance (IA) program within the command. The three basic position sensitivity levels/Position Designations:

Special-Sensitive (SS)/T5 or T5R; equivalent (SSBI, etc.) (IT Level I) - Potential for inestimable impact and/or damage.

Critical-Sensitive (CS)/T5 or T5R; equivalent (SSBI, etc.) (IT Level I) - Potential for grave to exceptionally grave impact and/or damage.

Noncritical Sensitive (NCS)/T3 or T3R; equivalent (ANAC/ANACI) (IT Level II) - Potential for some to serious impact and/or damage.

Investigative requirements for each category vary, depending on the role and whether the individual is a U.S. civilian contractor or a foreign national. The Contractor PM will assist the Government Project Manager or COR in determining the appropriate IT Position Category assignment for all contractor personnel.

As required by National Industrial Security Program Operating Manual (NISPOM) Chapter 1, Section 3, contractors are required to report certain events that have an impact on: 1) the status of the facility clearance (FCL), 2) the status of an employee's personnel clearance (PCL); may indicate the employee poses an insider threat, 3) the proper safeguarding of classified information, 4) or an indication that classified information has been lost or compromised. Contractors working under NIWC Pacific contracts will ensure information pertaining to assigned contractor personnel are reported to the Contracting Officer Representative (COR)/Technical Point of Contact (TPOC), the Contracting Specialist, and the Security's COR in addition to notifying appropriate agencies such as Cognizant Security Agency (CSA), Cognizant Security Office (CSO), or Department Of Defense Central Adjudication Facility (DODCAF) when that information relates to the denial, suspension, or revocation of a security clearance of any assigned personnel; any adverse information on an assigned employee's continued suitability for continued access to classified access; any instance of loss or compromise, or suspected loss or compromise, of classified information; actual, probable or possible espionage, sabotage, or subversive information; or any other circumstances of a security nature that would affect the contractor's operation while working under NIWC Pacific contracts.

IV. INTELLIGENCE OVERSIGHT

For any contractor personnel conducting Intelligence or Intelligence-related activities or supporting those efforts under Department of Defense authorities shall report any Questionable Intelligence Activity (QIA), Significant, or Highly Sensitive

Matter (S/HSM) to the Naval Information Warfare Systems Command Intelligence Oversight Program Manager or Senior Intelligence Officer.

Questionable Intelligence Activity (QIA): Any Intelligence or Intelligence-related activity when there is reason to believe such activity may be unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or applicable DoD policy governing that activity.

Significant or Highly Sensitive Matter (S/HSM): An Intelligence or Intelligence-related activity (regardless of whether the Intelligence or Intelligence-related activity is unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or DoD policy), or serious criminal activity by Intelligence personnel, that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of Intelligence activities. Such matters might involve actual or potential:

- Congressional inquiries or investigations
- Adverse media coverage
- Impact on foreign relations or foreign partners
- Systemic compromise, loss, or unauthorized disclosure of protected information.

V. CONTRACTOR COMPLIANCE WITH FOREIGN ENTRY REQUIREMENTS

Contractor personnel performing contracts outside of the United States must comply with the entry requirements of the respective geographic combatant command (GCC) and all applicable host nation procedures. These entry/clearance requirements are stipulated on a country-by-country basis in the Electronic Foreign Clearance Guide (EFCG), located at https://www.fcg.pentagon.mil. Compliance with the EFCG is required for all contractor personnel traveling outside of the United States in support of this contract. Contractor personnel are responsible for ensuring they obtain access to the EFCG by requesting a username and password at https://www.fcg.pentagon.mil, and that all foreign entry requirements are met.

VI. TRADEMARK RIGHTS (NEW PROGRAM)

The contractor shall not assert any claim, in any jurisdiction, based on trademark or other name or design-based causes of action that are based on rights the contractor believes it has in the term(s) such as names, words, acronyms, symbols, logos, seals, emblems used or intended to be used by the DoN acquisition programs addressed in this contract's statement of work or performance work statement (the "Designation(s)"), against the Government or others authorized by the Government to use the Designation(s) (including the word(s), name, symbol, or design) acting within the scope of such authorization (i.e. claims for trademark infringement, dilution, trade dress infringement, unfair competition, false advertising, palming off, passing off, or counterfeiting). Such authorization shall be implied by the award of a Government contract to any party for the manufacture, production, distribution, use, modification, maintenance, sustainment, or packaging of the products and services identified under this contract, and the scope of such implied authorization is defined as the use of the Designation(s) in performance under such contract by the prime contractor and its subcontractors and suppliers at any tier. In all other cases, the scope of the authorization will be defined by the Government in writing.

The contractor shall notify the contracting officer at least 30 days before asserting rights in, or filing an application to register, any one of the Designation(s) in any jurisdiction within the United States. Any such notification shall be in writing and shall identify the Designation(s) (including the word(s), name, symbol, or design), provide a statement as to its intended use(s) in commerce, and list the particular classes of goods or services in which registration will be sought.

VII. TRADEMARK RIGHTS (OLD PROGRAM)

The contractor shall not assert any claim, in any jurisdiction, based on trademark or other name or design-based causes of action that are based on rights the contractor believes it has in the term(s) such as names, words, acronyms, symbols, logos, seals, emblems used or intended to be used by the DoN acquisition programs addressed in this contract's statement of work or performance work statement (the "Designation(s)"), against the Government or others authorized by the Government to use the Designation(s) (including the word(s), name, symbol, or design) acting within the scope of such authorization (i.e. claims for trademark infringement, dilution, trade dress infringement, unfair competition, false advertising, palming off, passing off, or counterfeiting). Such authorization shall be implied by the award of a Government contract to any party for the manufacture, production, distribution, use, modification, maintenance, sustainment, or packaging of the products and services identified under this contract, and the scope of such implied authorization is defined as the use of the Designation(s) in performance

under such contract by the prime contractor and its subcontractors and suppliers at any tier. In all other cases, the scope of the authorization will be defined by the Government in writing.

VIII. CONTRACTOR NOTIFICATION – AWARENESS OF EXPECTATIONS

Contractor personnel must adhere to all current DoD, SECNAV, OPNAV, and NIWC Pacific instructions related to foreign travel.

Contractor personnel are reminded of their obligation to safeguard the vital relationship our Nation has with Foreign Countries. This includes personal conduct while performing under the contract and on one's personal time because, at all times, you are viewed by our partners as a representative of the United States, our Navy, and NAVWAR. Therefore, professional, courteous, and culturally aware conduct is necessary at all times. Inappropriate conduct, and especially intoxication and criminal behaviors, will not be tolerated. An all too common nexus for personnel misconduct while on travel is irresponsible consumption of alcohol. Intoxication increases your vulnerability to crime, injury, arrest, terrorism and espionage.

While traveling on official business, representing and performing in support of NAVWAR's mission, all personnel, including military, civilian and contractors, are expected to act in a professional and responsible manner. In order to promote effective relationships with business partners and allied nations, it is incumbent on contractor personnel to follow local laws and employ courteous and culturally aware behavior. Inappropriate conduct may jeopardize important relationships for the United States Navy, NAVWAR, NIWC Pacific and NIWC Atlantic, and will not be tolerated.

In all cases, contractors are reminded of their responsibilities under FAR Subpart 3.10, Contractor Code of Business Ethics and Conduct, and specifically FAR 3.1002, which requires contractors to conduct themselves with the highest degree of integrity and honesty.

Additionally, in accordance with FAR 3.1003(a)(2), contractors may be suspended and/or debarred for failing to timely disclose to the Government, in connection with the award, performance, or closeout of this contract or any subcontract thereunder, credible evidence that a principal, employee, agent, or subcontractor of the contractor has committed—

- A violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code; or
- A violation of the civil False Claims Act (31 U.S.C. 3729-3733).